destruction of classified electronic media and processing equipment components may be obtained by submitting all pertinent information to the National Security Agency/Central Security Service, Directorate for Information Systems Security, Fort Meade, MD 20755. Specifications concerning appropriate equipment and standards for the destruction of other storage media may be obtained from the GSA.

§ 2001.47 Loss, possible compromise or unauthorized disclosure [4.1, 4.2].

(a) *General.* Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) *Cases involving information originated by a foreign government or another U.S. government agency.* Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise.

(c) *Inquiry/investigation and corrective actions.* Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) *Department of Justice and legal counsel coordination.* Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with—

(1) The Department of Justice, and

(2) The legal counsel of the agency where the individual responsible is assigned or employed.

§ 2001.48 Special access programs [4.3].

(a) *General.* The safeguarding requirements of this Directive may be enhanced for information in Special Access Programs (SAP), established under the provisions of Section 4.3 of E.O. 12958, as amended, by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) *Significant interagency support requirements.* Agency heads must ensure that a Memorandum of Agreement/Understanding (MOA/MOU) is established for each Special Access Program that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

§ 2001.49 Telecommunications automated information systems and network security [4.1, 4.2].

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Index of National Security Telecommunications and Information Systems Security Issuances (NSTISSI) and Director of Central Intelligence Directive (DCID) 6/3.

§ 2001.50 Technical security [4.1].

Based upon the risk management factors referenced in § 2001.40 of this directive agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures (TSCM) and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, entitled Tempest Countermeasures for Facilities, and SPB Issuance 6–97, entitled